REMARKS

Claims 6-12, 14, 16, 18 and 20 stand rejected under 35 U.S.C. 102(b) as being anticipated by Downs et al. (U.S. Patent No. 6,226, 618). In response, Applicants traverse the rejection as it applies to independent claims 6, 12, 14, 16, 18, 20, and their respective dependent claims because Downs fails to disclose (or suggest) attach/detach key information on a hardware key which can be attached to and detached from a processing device. Applicants traverse the rejection as it applies to independent claim 14 because Downs fails to disclose (or suggest) a recording medium on which device identification information is fixedly recorded, a hardware key connection means for reading attach/detach key information that includes the identification information specifying a device, and a hardware key storing the attach/detach key information when the hardware key is attached.

Downs is directed to an electronic content delivery system and discloses a method and apparatus for securely providing data to a user's system. However, unlike the present invention, Downs does not disclose or suggest using a hardware key. The Examiner asserts in the outstanding Office Action that encrypted Content 113, digital content-related data or metadata, and encrypted keys that are packed in SCs (Secure Containers) by a SC Packer Tool and stored in a content hosting site and/or promotional website for electronic distribution corresponds to the hardware key of the present invention. However, the control of Content usage is software based, and not hardware based like the present invention.

More specifically, attach/detach key information issuing means 91 of the present invention generates attach/detach key information 91a including device

identification information 91b and an attach/detach key-specific encryption key 91c (see Applicants' specification, page 31, line 26 – page 32, line 3). The device identification information 91b is fixedly recorded on a recording medium 94a in a processing device 94 (see Applicants' specification page 32, lns. 3-6). The attach/detach key information 91a is recorded onto a hardware key 96, which can be attached to and detached from the processing device 94 (see Applicants' specification page 32, lns. 8-11). The hardware key 96 may then be given to a user of the processing device 94.

To access encrypted software using the present invention, the user must attach the hardware key 96 to the processing device 94. Once the hardware key 96 is attached, hardware key attachment means 94e reads the attach/detach key information 91a from the hardware key (see Applicants' specification page 33, lns. 4-6). Identification determining means 94c determines whether the device identification information 91b read from the hardware key 96 is the same as the device identification information recorded on the recording medium 94a (see Applicants' specification page 33, lns. 11-15). If it is determined that the two sets of information are the same, software decrypting means 94d decrypts encrypted software 99b using a software decryption key 98a decrypted by license information decrypting means 94b (see Applicants' specification page 33, lns. 15-20).

Downs, however, is silent regarding generating attach/detach key information on a hardware key, which can be attached, and in particular attached to and detached from a processing device. The Examiner asserts that control of the Content by a Clearinghouse is equivalent to a hardware key. However, issuance of a

key in Downs is based solely on software usage restrictions, and not the device identification information.

More specifically, as taught in Downs at column 7, lines 41-55, the control of Content usage is enabled through an End-User Player Application 195 running on an End-User Device(s). The application embeds a digital code in every copy of the Content that defines the allowable number of secondary copies and play backs. Digital watermarking technology generates digital code, keeps the digital code hidden from other End-User Player Applications 195, and makes a digital watermark resistant to alteration attempts. When the Digital Content is accessed in a compliant End-User Device(s), the End-User Player Application 195 reads the watermark to check the use restrictions and updates the watermark as required. If the requested use of the content does not comply with the use's conditions, the End-User Device(s) will not perform the request. Accordingly, issuing a key and allowing use of the data is based solely on use restrictions in the watermark, and not device identification information.

For all the above reasons, withdrawal of the §102(b) rejection of claims 6-12, 14, 16, 18 and 20 is respectfully requested.

Claim 13 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Downs in view of Johnson et al. (U.S. Patent No. 5,859,935). In response, Applicants traverse the rejection for the reasons recited above with respect to the rejection of independent claim 14.

The deficiencies of Downs are noted above. Johnson also fails to overcome the deficiencies of Downs. Johnson is merely cited for teaching a

determination of sameness and that a verification of sameness must be performed before an action of transferring data can take place. Johnson fails to disclose or suggest a hardware key storing attach/detach key information when the hardware key is attached. For this reason, withdrawal of the §103(a) rejection of claim 13 is respectfully requested.

For all of the foregoing reasons, Applicants submit that this Application is in condition for allowance, which is respectfully requested. The Examiner is invited to contact the undersigned attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By 
Joseph P. Fox
Registration No. 41,760

October 24, 2007
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
(312) 360-0080
Customer No. 24978